

IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method of attempting to provide virus protection for  
~~operating a filer~~ including the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes  
scanning said object for viruses using a combination of vendors' products ~~encrypting said object~~;

responding to said request, wherein said step of responding includes delivery of a  
response to said user.

2. (Original) The method of claim 1, wherein said request is in an electronic form.

3. (Original) The method of claim 1, wherein said object is a file.

4. (Previously Amended) The method of claim 3, wherein said step of processing said  
request further includes the steps of:

creating an access path from said filer to a processing cluster;

processing said file in said processing cluster; and

generating a report responsive to said processing of said file in said processing cluster.

5. (Original) The method of claim 4, wherein said step of creating an access path includes sending the ID and path of said file from said filer to said processing cluster.

6. (Original) The method of claim 5, wherein said step of sending is accomplished using non-uniform memory access.

7. (Original) The method of claim 5, wherein said step of sending is accomplished using a communications network.

8. (Original) The method of claim 5, wherein said step of sending is accomplished using a direct connection.

9. (Original) The method of claim 4, wherein said step of processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

10. (Original) The method of claim 4, wherein said step of processing of said file is accomplished in parts by more than one device in said processing cluster.

11. (Previously Amended) The method of claim 4, wherein all files stored on said filer are encrypted in a logical continuous manner.

12. (Previously Amended) The method of claim 4, wherein said report contains a set of status data relating to said processing of said file.

13. (Original) The method of claim 12, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

14. (Original) The method of claim 13, wherein said report is transferred to said filer.

15. (Original) The method of claim 14, wherein said report is stored in a first database.

Claims 16-17 (Canceled).

18. (Previously Amended) The method of claim 3, wherein said delivery of a response is said file.

19. (Previously Amended) The method of claim 3, wherein said delivery of a response includes notification to said user that said file is unavailable.

20. (Previously Amended) The method of claim 4, wherein said step of responding to said request includes sending said user a copy of said report.

21. (Currently Amended) An apparatus for attempting to provide virus protection  
~~operating a filer~~ including:

means for receiving at a first location a request from a user for an object;

means for processing said request at a second location, wherein said means for processing includes means for scanning said object for viruses using a combination of vendors' products ~~encrypting said object~~;

means for responding to said request, wherein said means for responding includes delivery of a response to said user.

22. (Original) The apparatus of claim 21, wherein said object is a file.

23. (Previously Amended) The apparatus of claim 22, wherein said means for processing said request further includes:

means for creating an access path from said filer to a processing cluster;

means for processing said file in said processing cluster; and

means for generating a report responsive to said processing of said file in said processing cluster.

24. (Original) The apparatus of claim 23, wherein said means for creating an access path includes means for sending the ID and path of said file from said filer to said processing cluster.

25. (Previously Amended) The apparatus of claim 24, wherein said sending is accomplished using non-uniform memory access.

26. (Previously Amended) The apparatus of claim 24, wherein said sending is accomplished using a communications network.

27. (Previously Amended) The apparatus of claim 24, wherein said sending is accomplished using a direct connection.

28. (Previously Amended) The apparatus of claim 23, wherein said processing of said file is performed by said processing cluster in a round robin fashion for subsequent files received.

29. (Previously Amended) The apparatus of claim 23, wherein said processing of said file is performed on atomic units of said file by more than one device in said processing cluster.

30. (Previously Amended) The apparatus of claim 23, wherein all files stored on said filer are encrypted in a logical continuous manner.

31. (Previously Amended) The apparatus of claim 23, wherein said report contains a set of status data relating to said processing of said file.

32. (Original) The apparatus of claim 31, wherein said status data includes at least one data element identifying the presence or non-presence of a virus in said file.

33. (Original) The apparatus of claim 31, wherein said report is transferred to said filer.

34. (Original) The apparatus of claim 33, wherein said report is stored in a first database.

Claims 35-36 (Canceled).

37. (Previously Amended) The apparatus of claim 22, wherein said delivery of a response is delivery of said file.

38. (Previously Amended) The apparatus of claim 22, wherein said delivery of a response includes delivery of notification to said user that said file is unavailable.

39. (Previously Amended) The apparatus of claim 23, wherein said responding to said request includes sending said user some portion of said report.

40. (Currently Amended) A method of attempting to provide virus protection in a client-server environment, comprising the steps of:

receiving a request at a server for a file;

sending, from the server, an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products;

receiving, at the server, an indication from the scanning devices as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send ~~; wherein communication between the server and the cluster of scanning devices is performed using non-uniform memory access.~~

41. (Previously Amended) A method as in claim 40, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses.

42. (Previously Presented) A method as in claim 40, wherein the request is received from and the file is sent to a client device.

43. (Previously Presented) A method as in claim 40, wherein the server is a web server.

Claim 44 (Canceled).

45. (Previously Presented) A method as in claim 44, wherein the cluster of devices is a cluster of interconnected personal computers.

Claims 46-56 (Canceled).

57. (Currently Amended) A server that attempts to provide virus protection ~~encryption~~ services in a client-server environment, comprising:

a communication link to client devices;

mass storage for files; and

a processor that executes instructions in order to send requested files to the client devices, the instructions also including instructions (a) to receive a request for a file, (b) to send an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products ~~an encrypting device that encrypts the file~~, and (c) to respond to the request by sending the file.

58. (Canceled).

59. (Previously Presented) A server as in claim 57, wherein the request is received from and the file is sent to a client device.



60. (Previously Presented) A server as in claim 57, wherein the server is a web server.

61. (Cancelled)

62. (Currently Amended) A server as in claim 57 ~~61~~, wherein the cluster of devices is a cluster of interconnected personal computers.

Claims 63-73 (Canceled).

74. (Currently Amended) Storage containing information including instructions, the instructions executable by a processor to attempt to provide virus protection in a client-server environment, the instructions comprising the steps of:

receiving a request at a server for a file;

sending, from the server, an identifier for the file to a cluster of scanning devices that scan the file for viruses using a combination of vendors' products;

receiving, at the server, an indication from the scanning devices as to whether or not the file is safe to send from the server; and

responding to the request by sending the file if the indication is that the file is safe to send;

wherein communication between the server and the cluster of scanning devices is performed using non-uniform memory access.

75. (Previously Amended) Storage as in claim 74, wherein the scanning devices indicate that the file is safe to send if the scanning devices determine that the file is not infected with any viruses.

76. (Previously Presented) Storage as in claim 74, wherein the request is received from and the file is sent to a client device.

77. (Previously Presented) Storage as in claim 74, wherein the server is a web server.

Claim 78 (Canceled).

79. (Previously Amended) Storage as in claim 74, wherein the cluster of devices is a cluster of interconnected personal computers.

Claims 80-90 (Canceled).

91. (Currently Amended) Storage containing information including instructions, the instructions executable by a processor to provide virus protection ~~operate a file~~, the instructions comprising the steps of:

receiving at a first location a request from a user for an object;

processing said request at a second location, wherein said step of processing includes scanning said object for viruses using a combination of vendors' products ~~encrypting said object;~~  
responding to said request, wherein said step of responding includes delivery of a response to said user.